ABSTRACT

Storing events to enhance intrusion detection in networks is described. In one exemplary implementation, an event is received. The event includes a data section containing a set of strings each having an event field. A definition table is referenced to determine locations of event fields in the data section of the event. The event fields are stored in a database record corresponding to event field locations referenced from the definition table.